文章编号:1000－2367(2018)05－0110－08 DOI:10.16366/j.cnki.1000－2367.2018.05.018

一种动态猫映射混沌图像加密算法

王鲜芳[a,b], 王晓雷[a], 王俊美[a], 李名[a]

(河南师范大学 a.计算机与信息工程学院; b.计算智能与数据挖掘河南省高校工程技术研究中心,河南 新乡 453007)

摘 要:针对传统猫映射存在周期性以及位置(0,0)处像素始终固定导致的安全隐患,提出了一种基于动态猫映射的图像加密算法.首先把密钥经过 md5 变换后得到一个十六进制字符串,利用该字符串,获取动态猫映射的分块边界参数,并通过 md5 的随机性构建扩散阶段需要的 S 盒.在置乱阶段,将猫映射置乱参数与明文图像结合起来,进行动态猫映射,得到置乱图像.在扩散阶段,每个像素值用 S 盒进行扩散时,结合相邻像素值,形成雪崩效应.最后进行仿真实验,结果表明提出的加密算法能满足图像加密的安全性需求,不仅改善了传统猫映射存在的缺陷,而且具有更好的加密效果.

关键词:动态猫映射;混沌;图像加密;S 盒

中图分类号:TP309.7 **文献标志码**:A

研究图像加密算法是当今信息安全领域重要的课题,现有图像加密算法主要有空域图像加密[1－4]和变换域图像加密[5].空域图像加密主要通过位置和灰度值变换来实现,变换域图像加密通过频域处理的方式来改变图像中不同频率的分量,不对应于空域中的单个像素.空域图像加密一般包括置乱和扩散两个阶段.在置乱阶段,主要是对图像的像素位置进行替换,猫映射是一种常用的置乱算法[6－10],然而该算法存在以下问题:(1)周期性问题;(2)图像起始位置(0,0)处像素值在置乱过程中始终不移动导致加密策略存在安全隐患.针对周期性问题,文献[4]在猫映射中加入多个混沌序列,然而该加密方案仍然存在安全漏洞,这一安全漏洞已经被文献[11]成功破解.针对传统猫映射在(0,0)处像素值始终不移动的问题,文献[12]把猫映射从二维扩展到了三维,取得了较好的加密效果,但是整个加密算法的计算代价过大.在扩散阶段,主要是修改图像的像素值以改变图像的灰度值直方图分布等统计信息,目前所采用的方法之一是使用 S 盒[13－17].混沌系统由于具有高度的伪随机性,因此应用范围较为广泛.文献[18]提出了一种基于改进混沌粒子群算法的多源独立微网多目标优化方法,利用混沌系统特有的遍历性来实现全局最优,文献[13]使用混沌系统产生非线性 S 盒,文献[14]引入混沌序列产生多个 S 盒并且进行多轮 S 盒替换, 文献[16]提出了一种基于 S8 替换盒和 NAC 混沌映射的加密算法.S 盒是加密算法中很重要的非线性部分,其非线性程度直接影响着加密效果的好坏.一般情况下,一个混沌系统的维度越高,其表现的随机性就越强.文献[19]提出了一种四维混沌与分数傅里叶变换的图像加密方案,具有很好的加密效果,但是较高维度的混沌系统对计算机系统的资源消耗较大.文献[20]提出了一种基于混沌序列的 DWT 数字水印算法,相比文献[19]来讲,该算法对计算资源的消耗则比较小.故在设计加密方案时候,为了使算法的执行时间最少,应该尽可能地减少浮点型数据的运算操作.

针对猫映射置乱图像存在的安全问题,本文设计了一种基于动态猫映射的图像加密算法.首先,对密钥进行 md5 变换,可以将任意形式的输入变换成一个固定长度为 32 位的十六进制字符串.然后,使用该字符串后 16 位进行边界处理产生用于动态猫映射的置乱参数,结合灰度值对明文图像进行动态猫映射,达 到 置

收稿日期:2017-12-06;**修回日期**:2018-04-25.

基金项目:国家自然科学基金(61173071;61602158);河南省高校创新人才支持计划项目(2012HASTIT011);中国博士后科学基金资助项目(2016M600030).

作者简介(通信作者):王鲜芳(1969－),女,河南洛阳人,河南师范大学教授,博士,主要研究方向为人工智能与模式识别,E-mail:121113@htu.edu.cn.

乱图像、避免周期性问题的目的；使用其前 16 位和 Logistic 映射生成很少的数值，经过 md5 变换后再处理得到 S 盒，以降低计算资源的开销和计算精度对结果的影响.用 S 盒对动态猫映射置乱后的图像进行扩散，引入雪崩效应，以抵抗差分攻击.最后通过仿真实验，证明本文提出加密算法的有效性.

1　动态猫映射图像加密原理

图像加密方案一般由两个步骤组成：置乱和扩散.在置乱阶段，置乱图像的像素位置.置乱后的图像，由于像素值无任何改变，故图像的灰度值分布等统计信息也不变，因此增加扩散阶段以提高图像加密的安全性.在扩散阶段，图像的像素值被修改，掩盖掉原有的统计特征，完成全部加密过程.本文提出的动态猫映射图像加密原理如图 1 所示.

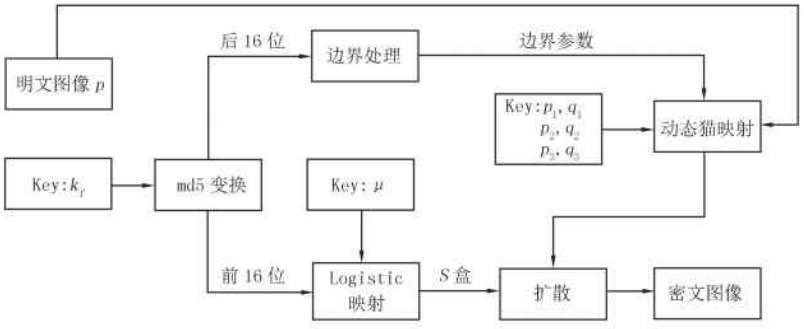

图 1　加密算法原理图

(1)预处理.先对输入密钥 k_f 进行 md5 变换得到一个固定长度为 32 位的十六进制字符串.然后利用后 16 位和边界处理产生用于动态猫映射的置乱参数；利用前 16 位和 Logistic 映射产生用于扩散图像的 S 盒；

(2)置乱加密.利用后 16 位结合边界参数，结合灰度值对明文图像进行关联，使用动态猫映射方案进行置乱加密，得到置乱图像；

(3)扩散加密.利用前 16 位和 Logistic 映射得到的 S 盒对动态猫映射置乱后的图像进行扩散，形成雪崩效应，以抵御选择明文攻击，提高加密效果.

2　动态猫映射图像加密过程

本文设计的加密过程主要分为 3 个步骤，分别为预处理、动态猫映射置乱和 S 盒扩散加密.

2.1　预处理

待处理的明文图像大小为 $N \times N$，加密用的密钥为 $k_f, \mu, p_1, q_1, p_2, q_2, p_3, q_3$，其中 k_f 为任意输入，μ 是 Logistic 映射的控制参数并且 $\mu \in (3.67, 4)$，其余为整数作置乱参数使用.首先对 k_f 按照以下步骤进行预处理，得到加密过程需要用到的置乱参数和 Logistic 映射的初始值.后者联合控制参数 μ 生成混沌序列，然后经过 md5 变换，最终生成 S 盒.

(1)md5 变换及边界处理.对密钥 k_f 进行 md5 变换，得到一个 32 位的十六进制字符串 k_m.md5 变换的一个特点是将任意长度的报文映射为固定长度的 Hash 码.它具有抗弱碰撞以及抗强碰撞等特性[21]，能够较好地掩藏和映射原文信息.如对一组输入信息“sdgfdg55”进行 md5 变换得到：36e90475f550c4a33cd57836d27bb129.

取 k_m 的后 16 位字符当作十六进制字符串，十进制后表示为 k_a，按照(1)式得到动态猫映射的边界参数 b_p，

$$p_p = k_a/(16^{16}), b_p = 0.5 + 0.5 \times p_p. \tag{1}$$

对于 md5 的变换结果，按每 2 个连续字符当作一个十六进制形式的数，分别是：36，e9，04，75，f5，50，c4，a3，3c，d5，78，36，d2，7b，b1，29.转换成十进制数就是 54，233，4，117，245，80，196，163，60，213，120，54，210，

123,177,41.这些数的取值范围为像素值范围,在数量上等价于一个 16×16 的 S 盒的 1/16.只需要用混沌映射产生 16 个随机值,然后使用 md5 变换能简单高效地生成图像扩散阶段的 S 盒.md5 变换过程不进行浮点数运算,具有计算速度快等优点,能简单高效地生成图像扩散阶段所需的 S 盒.

(2)Logistic 映射.Logistic 映射[22]是研究动力系统、混沌、分形等复杂系统行为的一个经典模型,又叫 Logistic 迭代,其基本模型如(2)式所示.本方案取 k_m 的前 16 个字符当作十六进制字符串,十进制后表示为 k_p.利用 Logistic 映射产生随机序列,从随机位置 r_p 处开始依次取 16 个数值,经过 md5 变换及后期处理得到用于扩散的 S 盒.

$$t_{n+1}=\mu t_n(1-t_n), \tag{2}$$

$$r_p=\sum_{i=1}^{32}(k_m)_i, \tag{3}$$

$$t_0=k_p/(16^{16}), \tag{4}$$

(3)式中 $(k_m)_i$ 表示 k_m 的第 i 个字符的十进制值.

利用(4)式得到 Logistic 混沌映射的初始值 $_t0$,并用于(2) 式得到一个随机序列,这里 n 为迭代的次数,t_n 和 t_{n+1} 分别为当前值和下一个值,$t_n,t_{n+1}\in(0,1)$,μ 为控制参数,为了保证映射得到的 t_n 始终在(0,1)内,需要 $\mu\in(0,4)$.当变化不同的参数 μ 的时候,该方程会展现出不同的动力学极限行为.当 $\mu\in(3.67,4)$ 时,整个系统会呈现出混沌特性.

2.2 动态猫映射置乱

猫映射也称为 Arnold 映射,是一种常用的置乱算法,由俄国数学家弗拉基米尔·阿诺德[6]提出,它是一种在有限区域内进行反复折叠、拉伸变换的混沌映射方法.数字图像猫映射置乱可以表述为:

$$\begin{bmatrix}x_{n+1}\\y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & p\\ q & pq+1\end{bmatrix}\begin{bmatrix}x_n\\y_n\end{bmatrix}\bmod N, \tag{5}$$

在(5)式中,参数 p 和 q 均为正整数,是猫映射的置乱参数.(x_n,y_n) 和 (x_{n+1},y_{n+1}) 分别表示置乱前后的像素位置.这种猫映射算法在对图像进行置乱加密时存在周期性,即图像经过若干次迭代加密后,会完全变换成明文图像,这就使得攻击者可以仅通过反复迭代来恢复明文.从(5)式还可以发现,该算法的(0, 0)处位置的像素值始终没有移动,这会成为加密方案的一个隐患.

为了解决传统猫映射存在的周期性等问题,本文设计了一种动态猫映射的加密算法.该算法的原理是使猫映射的置乱参数随明文动态发生变化,从而避免猫映射由于周期性带来的安全缺陷.具体步骤如下:

(1)参数初始化.将明文图像按图 2 方式分块.令 $AB=AC=N$,并且有 $AE=AR=DH=DV$. 令:

$$AE=\lceil b_p\times N\rceil, \tag{6}$$

(6)式中$\lceil\ \rceil$表示向上取整.

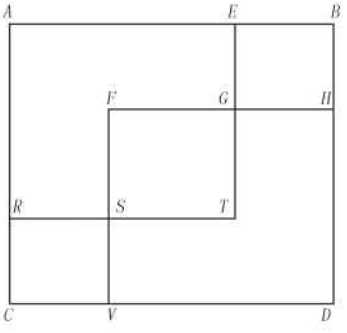

图 2 图像分割示意图

(2)置乱参数动态变化.为了改善猫映射置乱算法的周期性带来的安全缺陷,每次置乱前,先使用明文图像本身对置乱参数进行变换,再将变换后的参数用于置乱加密.具体过程如下:

首先对图 2 的 $ARTE$ 部分进行猫映射置乱加密,该部分对应的原始置乱参数为 p_1,q_1.用 δ 表示 $ARTE$ 部分所有像素值之和,对 p_1 和 q_1 进行如下变换.

$$pp_1=p_1\oplus\lceil\delta/N/N\rceil\oplus(\delta\bmod 32),qq_1=q_1\oplus\lceil\delta/N/N\rceil\oplus(\delta\bmod 32), \tag{7}$$

(7)式中表示异或运算.

得到新的置乱参数 pp_1 和 qq_1.对于 $DVFH$ 部分,对应的置乱参数是 p_2 和 q_2,经过同样处理,得到新的置乱参数 pp_2 和 qq_2.最后,对于 $ABDC$ 整体,对应的置乱参数是 p_3 和 q_3 同样处理可得到新的置乱参数 pp_3 和 qq_3.

(3)动态猫映射置乱.为了改进(0, 0)处位置的像素值始终没有移动而带来的安全隐患,首先对传统猫

映射进行改进,

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \left(\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} + \lfloor p_p \times N \rfloor \right) \bmod N. \tag{8}$$

(8)式中 p_p 来自(1)式,$\lfloor\ \rfloor$表示向下取整.

针对解决传统猫映射存在的周期性问题,本文使用新得到的 3 组置乱参数,pp_1 和 qq_1,pp_2 和 qq_2,pp_3 和 qq_3,分别对 $ARTE$ 部分、$DVFH$ 部分和 $ABDC$ 部分使用(8) 式进行猫映射置乱加密.需要注意的是,为了实现置乱参数的动态变化,需要先对 $ARTE$ 部分执行过置乱后,再对 $DVFH$ 部分进行置乱参数更新和使用新参数进行置乱操作.

2.3 S 盒扩散加密

利用预处理中得到的 S 盒,对置乱图像进行扩散加密.置乱图像用 p 表示,S 盒用 s 表示.

$$p_{tm} = p_{(i+1) \bmod (N \times N)} + 1, p_i = p_i \oplus s_{p_{tm}}, \tag{9}$$

(9)式中,p_i 表示图像 p 中 i 位置处像素点的值,$s_{p_{tm}}$ 表示 S 盒中 p_{tm} 处的值,$i = 1,2,3,\cdots,N^2$. 为了更好地隐藏明文图像(0,0)处像素值的信息,将扩散过程进行至少 2 轮.

3　解密过程

输入解密密钥:k_f, μ, p_1, q_1, p_2, q_2, p_3, q_3,先预处理 k_f,生成动态猫映射的边界参数和扩散阶段需要的 S 盒.把密文图像逆向进行扩散操作,得到置乱图像.然后根据边界参数和 3 组对应的置乱参数对置乱图像逆向进行动态猫映射,即可完成解密操作.具体步骤如下:(1) 预处理 k_f,得到动态猫映射的边界参数和 S 盒;(2)按照加密方案中的扩散方法,对密文图像逆向进行,得到明文图像的置乱图像;(3)联合动态猫映射的边界参数,对置乱图像进行逆向的动态猫映射,完成解密过程,$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \left(\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} + N - \lfloor p_p \times N \rfloor \right) \bmod N.$

4　实验过程、算法性能测试及结果分析

为了测试本文设计算法的性能,进行相关实验,并通过统计、差分攻击、相关性、信息熵、密钥灵敏度测试以及周期性测试等 6 个方面对加密效果进行分析.

4.1　实验过程及结果

选取大小为 256×256 的 Lenna 灰度图像,使用 k_f = sdgfdg55,$\mu = 3.732$,$p_1 = 2$,$q_1 = 3$, $p_2 = 1$,$q_2 = 7$, $p_3 = 3$,$q_3 = 6$,用本文设计的动态猫映射算法对图像进行加密操作.为了简化过程,本次实验进行 1 轮动态猫映射和 2 轮扩散加密.实验产生的 S 盒如表 1 所示,最终加密结果如图 3 和图 4 所示.

4.2　性能分析

4.2.1　统计分析

灰度值直方图描述了一幅图像的像素值分布情况,图像加密方案应该改变原始图像的像素值分布特征.如果密文图像的灰度值直方图不够平滑,对应的加密方案就容易受到唯密文攻击[1,20],即攻击者获取到一部分数据后,就能使用统计攻击快速地破解密文图像.明文

图 3　原始图像 (Lenna)

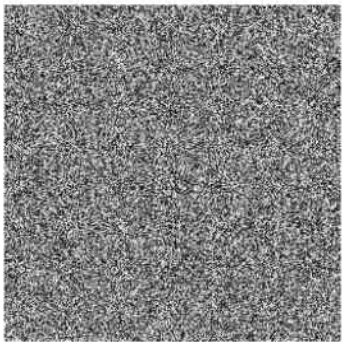

图 4　密文图像

图像和使用本文提出的算法加密后得到的密文图像,灰度值直方图分别如图 5 和图 6 所示.可以直观地看出,两幅图像的灰度统计值存在明显的差异,密文图像的灰度值分布比较平均,这说明算法的灰度扩散是有效的,能够有效地抵御唯密文攻击.

4.2.2 差分攻击分析

算法对明文的敏感性越强,抵御差分攻击的能力就越强.加密算法对明文的敏感性,常用的衡量指标为:像素数改变率(Number of Pixels Change Rate,NPCR),归一化像素值平均改变强度(Unified Average Changing Intensity,UACI).假设明文图像分别为 p_1 和 p_2,对应的密文图像为 c_1 和 c_2.定义一个运算 $V(i,j)$.如果两幅图像的(i,j) 坐标处像素点的值不同,则 $V(i,j)=1$,否则,$V(i,j)=0$. NPCR(简记 N_R)和 UACI(简记 U_I)是通过对比相应的密文图像运算得到,

$$N_R=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}V(i,j)}{M\times N}\times 100\%,U_I=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|c_1-c_2|}{2^8-1}}{M\times N}\times 100\%.$$

本实验使用 $k_f=$ 3cd57836d27bb129,明文图像的第 55 行第 1 列位置处像素值增大 1,其他参数不变,计算 N_R 和 U_I 值,结果依次是 0.996 5 和 0.334 5.对于 8 位灰度图像,其 N_R 与 U_I 的理想期望值分别为 0.996 1和 0.334 6.本次实验结果见表 2,其对应数据与理想期望值非常接近,相对文献[4],本方案的 N_R 值更高.虽然 U_I 略低,但也达到了安全标准的要求,表明了本文提出的算法能有效地抵御差分攻击.

表 1 实验生成的 S 盒

54	180	155	162	22	168	41	228	15	127	169	225	8	174	87	72
1	253	52	115	60	254	133	142	250	219	75	135	75	144	23	208
187	1	94	76	197	31	182	9	243	206	1	143	220	106	175	1
114	179	166	16	128	111	178	54	82	53	194	58	201	234	205	167
38	116	148	175	89	154	14	239	148	252	64	173	180	194	19	1
55	255	139	216	115	227	166	179	243	103	91	123	77	19	12	228
116	148	116	21	87	93	193	103	209	200	72	204	217	162	251	195
104	176	103	3	250	2	2	32	182	131	46	10	221	226	24	86
136	94	252	187	120	109	9	176	12	96	115	123	2	75	151	218
83	225	240	35	150	190	174	204	143	49	60	50	222	24	40	206
145	42	185	39	67	202	7	29	23	185	212	118	112	64	233	119
193	46	215	111	146	15	29	253	178	33	45	100	179	225	162	47
244	156	85	158	146	38	135	105	113	182	131	208	132	110	138	93
167	35	198	196	9	105	170	138	159	36	126	49	249	49	31	51
138	20	28	36	191	199	196	37	213	26	157	249	67	224	72	23
188	74	185	193	30	57	12	178	148	139	150	118	193	136	255	186

4.2.3 相关性分析

相关性揭示了图像中相像素点的值彼此相关的程度.从图像的水平方向、垂直方向和对角方向,各自选取一些相邻的像素点 (x,y),计算相关系数 r_{xy}. 相关系数的计算方法如下:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i,D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2, \tag{10}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)),r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{11}$$

利用(10)~(11)式对表 1 的 S 盒数值在水平方向、垂直方向、对角方向上计算它们之间的相关系数,计算结果如表 3 所示.从表 3 中可以看出,各方向的相关系数都在 0 附近,说明这些数值之间相关性很小,进而表明

这个 S 盒具有较强的随机性,能满足加密安全的需求.

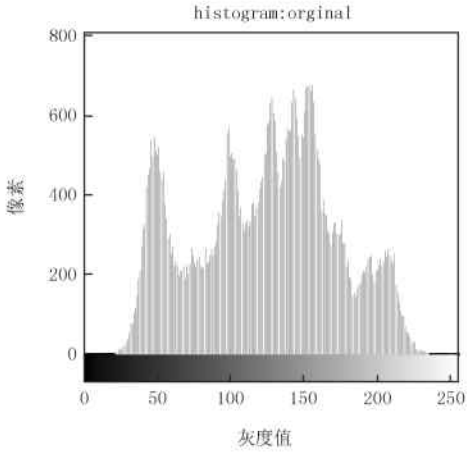

图 5　原始明文图像的灰度值直方图

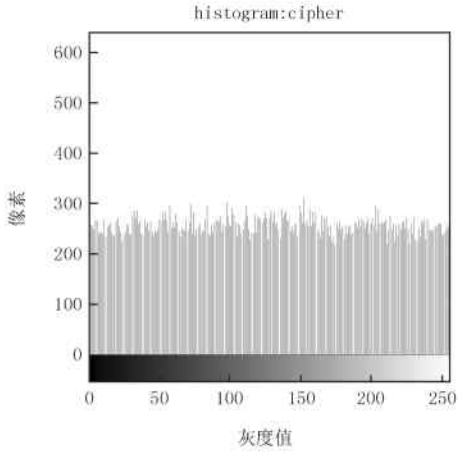

图 6　加密后密文图像的灰度值直方图

表 2　算法对明文的敏感性

方法	N_R	U_I
文献[8]	0.995 5	0.340 4
本文方法	0.996 5	0.334 5

表 3　S 盒数值的随机性分析

相关方向	相关系数
水平方向	−0.08
垂直方向	−0.20
对角方向	0.01

再利用(10)～(11)式对明文图像和密文图像的相邻像素在水平方向、垂直方向、对角方向上计算它们各自之间的相关系数,所得结果如表 4 所示.

表 4　相邻像素之间的相关性

相关比较	明文图像			密文图像		
	水平方向	垂直方向	对角方向	水平方向	垂直方向	对角方向
文献[8]	—	—	—	0.007 2	0.013 3	0.026 7
文献[16]	0.935 8	0.960 9	0.911 8	0.064 9	0.017 4	0.046 6
本文方法	—	—	—	0.003 0	0.002 3	0.003 7

从表 4 可以看出,该明文图像在水平方向、垂直方向和对角方向 3 个方向的相邻像素相关性都在 0.9 以上,而明文图像的相邻像素相关性变的非常低,这表明该算法增大了图像被非法恢复的难度,在相邻像素相关性方面,比文献[4,12]有更高的安全性.

4.2.4　信息熵

一幅图像如果有 L 种灰度值 m_i,其中 i 为 1 到 L 的正整数.各灰度值出现的概率分别为 $p(m_i)$,图像的信息熵计算过程如下,

$$H(m)=-\sum_{i=0}^{L-1}p(m_i)\log_2 p(m_i),\ \sum_{i=0}^{L-1}p(m_i)=1. \tag{12}$$

称 H 为图像的信息熵.图像的信息熵可以用来评估灰度值的分布.在灰度图像上(即 $L=2^8$),对于完全理想的随机图像,其信息熵等于 8.灰度图像的密文图像的信息熵越接近 8,则表示所使用的加密方案对暴力攻击的抵抗能力越强.对 Lenna 图像使用本方案加密,得到的密文图像的信息熵为 7.996 9,这个结果非常接近 8,表明本方案能够较好地抵抗暴力攻击.

4.2.5　密钥灵敏度测试

密钥的灵敏度是密钥发生微小改动所引起的密文图像的变化程度.密文图像变化得越明显,密钥的灵敏度越高.本次实验仅使 k_f 发生轻微改变,其他密钥保持不变的情况下,观察加密效果.具体过程为,分别对明

文图像使用“sdgfdg55”和“sdgfdg54”进行加密,依次得到密文图像 C_1 和 C_2.经过比较 C_1 和 C_2 相同位置的像素值,计算两幅密文图像的差异程度,结果为 99.62%.经过大量实验,微小的密钥变化均导致了密文图像的明显变化,因此本文的设计方案具有较高的密钥灵敏度.对使用 sdgfdg55 加密得到的 C_1 密文图像使用 sdgfdg54 来解密,则无法获取任何有效的明文信息,正确的解密成功结果和使用错误密钥解密失败的结果分别如图 7 和图 8 所示.

4.2.6 周期性测试

将明文图像用传统的猫映射算法和本文改进的动态猫映射算法分别进行 30 000 次迭代加密,记录实验结果并比较.用差异率来表示加密效果的性能,即统计密文图像和明文图像中对应位置上像素值不同的程度.如果出现 0,就说明密文图像和明文图像完全一样,出现了周期性.

图 7 正确的密钥解密图像

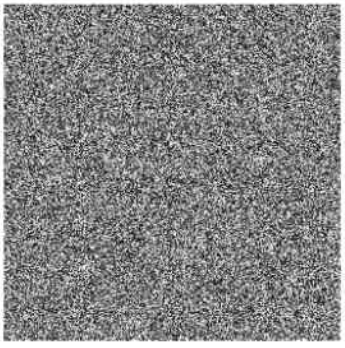

图 8 错误的密钥解密图像

表 5 本文方法与传统猫映射的置乱效果

加密算法	密文和明文的差异率		
	最小值	最大值	平均值
传统的猫映射	0.000 0	0.994 4	0.986 2
本文方法	0.992 5	0.994 7	0.993 7

实验结果表明,传统的猫映射在第 192 次迭代中就出现了周期性,而本文提出的动态猫映射并未在测试中观测到周期性缺陷.如表 4 所示,猫映射的置乱效果,与明文图像相比,存在差异率为 0.000 0 的情况,即密文和明文完全一样,存在安全缺陷.动态猫映射的最差置乱效果为 0.992 5 的差异率,不仅没有发现周期性,并且平均置乱效果比传统的猫映射更好.

5 结 论

针对传统猫映射存在周期性以及位置(0,0)处像素始终固定导致的安全隐患,提出了一种基于动态猫映射的图像加密算法.该算法首先通过对密钥进行 md5 变换,得到一个固定长度为 32 位的十六进制字符串,在置乱阶段,利用该字符串的后 16 位进行边界处理产生动态变化置乱参数,结合灰度值和关联明文图像进行动态猫映射.在扩散阶段,利用前 16 位和 Logistic 映射产生较少数量的随机值经过 md5 变换和相关处理后生成具有随机性能的 S 盒,并利用该 S 盒对动态猫映射置乱后的图像进行扩散,形成雪崩效应.最后进行相关实验,并在统计、差分攻击、相关性、信息熵、密钥灵敏度测试以及周期性测试等六个方面对加密效果进行分析,证明了本文设计的动态猫映射图像加密算法不但有效克服了传统猫映射存在的性能缺陷,还能够抵抗选择明文攻击,具有较高的效率、稳定性和安全性.本文的创新之处在于以下两个方面:(1)有效克服了传统的猫映射存在周期性、位置(0,0)处像素始终不移动等缺陷;(2)动态猫映射置乱阶段中,将加密方案与明文本身关联了起来,对选择明文攻击有较强的抵抗能力.

参 考 文 献

[1] Wang X,Zhang H L.A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems [J].Nonlinear Dynamics,2016,83(1/2):333-346.

[2] Devaraj P,Kavitha C.An image encryption scheme using dynamic S-boxes [J].Nonlinear Dynamics,2016,86(2):927-940.

[3] Belazi A,El-Latif A A A,Belghith S.A novel image encryption scheme based on substitution-permutation network and chaos [J].Signal Processing,2016,128:155-170.

[4] Tong X J.Design of an image encryption scheme based on a multiple chaotic map [J].Communications in Nonlinear Science & Numerical Simulation,2013,18(7):1725-1733.
[5] 刘钺.一种小波变换域图像加密技术 [J].计算机工程与应用,2010,46(19):157-159.
[6] Avaroglu E.Pseudorandom number generator based on Arnold cat map and statistical analysis [J].Turkish Journal of Electrical Engineering & Computer Sciences,2017,25(1):633-643.
[7] 彭嘉星，鲍芳.基于高维广义超混沌猫映射的彩色图像加密算法 [J].工业控制计算机,2016,29(7):74-75.
[8] 商凯，刘建东，张啸，等.整数非线性耦合映象格子模型及其性能分析 [J].计算机科学与探索,2017,11(3):389-395.
[9] 谢国波，邓华军.二次广义 cat 映射的混合混沌图像加密算法 [J].计算机工程与应用,2017.DOI:10.3778/j.issn.1002－8331.1703－0290.
[10] 闵祥参，张雪锋.基于多混沌系统的分组结构灰度图像加密算法 [J].西安邮电大学学报,2017,22(3):62-67.
[11] Liu H,Liu Y.Security assessment on block-Cat-map based permutation applied to image encryption scheme [J].Optics & Laser Technology,2014,56(1):313-316.
[12] 张燕，黄贤武，刘家胜.一种基于改进的混沌猫映射的图像加密算法 [J].计算机工程,2007,33(10):166-168.
[13] Venkatachalam S P,Vignesh R,Sathishkumar G A.An improved s-box based algorithm for efficient image encryption [C].//International Conference on Electronics and Information Engineering,Washington DC:IEEE Computer Society,2010:6 V1－428－V1－431.
[14] Wang D,Zhang Y B.Image Encryption Algorithm Based on S-boxes Substitution and Chaos Random Sequence [C].//International Conference on Computer Modeling and Simulation,Washington DC:IEEE Computer Society,2009:110-113.
[15] Xian Z H,Sun S L.Image Encryption Algorithm Based on Chaos and S-Boxes Scrambling [J].Advanced Materials Research,2011,171/172:299-304.
[16] Hussain I,Shah T,Gondal M A.An efficient image encryption algorithm based on S8 S-box transformation and NCA map [J].Optics Communications,2012,285(24):4887-4890.
[17] Jolfaei A,Wu X W,Muthukkumarasamy V.On the Security of Permutation-Only Image Encryption Schemes [J].IEEE Transactions on Information Forensics & Security,2015,11(2):235-246.
[18] 苏适，周立栋，陆海，等.基于改进混沌粒子群算法的多源独立微网多目标优化方法 [J].电力系统保护与控制,2017,45(23):34-41.
[19] 苏婷，董胜伟，吕志伟.四维混沌与分数傅里叶变换的图像加密方案[J].河南师范大学学报(自然版),2015(1):165-170.
[20] 林爱英，郑宝周，贾树恒.基于混沌序列的 DWT 数字水印算法 [J].河南师范大学学报(自然科学版),2011,39(3):157-161.
[21] Jiang J,Zhang X,Yu Y X,et al.Design of Internet of things transmission module based on md5 encryption algorithm [J].Transducer and Microsystem Technologies,2017.
[22] Mohamed M P,Abdul J S,Parameswaran B B.Medical Images are Safe - an Enhanced Chaotic Scrambling Approach [J].Journal of Medical Systems,2017,41(10):167.

A chaotic image encryption algorithm based dynamic cat map

Wang Xianfang[a,b], Wang Xiaolei[a], Wang Junmei[a], Li Ming[a]

(a.College of Computer and Information Engineering; b.Engineering Technology Research Center for Computing Intelligence & Data Mining of Henan Province,Henan Normal University,Xinxiang 453007,China)

Abstract: As the problem that traditional cat mapping is periodic and the position (0,0) is always fixed perplexes the security of information,an image encryption algorithm based on dynamic cat mapping is proposed.Firstly,the key is transformed by md5 to generate a hexadecimal string.This string is used to take the block boundary of the dynastic cat mapping.Meanwhile,the *S*-box which is needed in the diffusion phase is generated via the hexadecimal string.In the process of scrambling,the plain image is encrypted with scramble parameters by dynamic cat map.Then,the scrambling image is obtained.In the process of diffusion,the *S*- box is used with conjunction with the adjacent pixel value when the current pixel is processed so that the change of each pixel can cause the others' variation to form the avalanche effect.Finally,the simulate results show that the proposed encryption scheme satisfies the security requirements of image encryption,which not only avoids the disadvantage of periodicity in property,but also has a better performance than traditional cat mapping.

Keywords: dynamic cat mapping; chaotic; image encryption; *S*-box

[责任编校　陈留院]